PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-288275

(43)Date of publication of application : 10.10.2003

(51)Int.Cl. G06F 12/14
G06F 15/00
G06K 17/00
G06K 19/00

(21)Application number : 2002-093169

(22)Date of filing : 28.03.2002

(71)Applicant : FUJITSU LTD

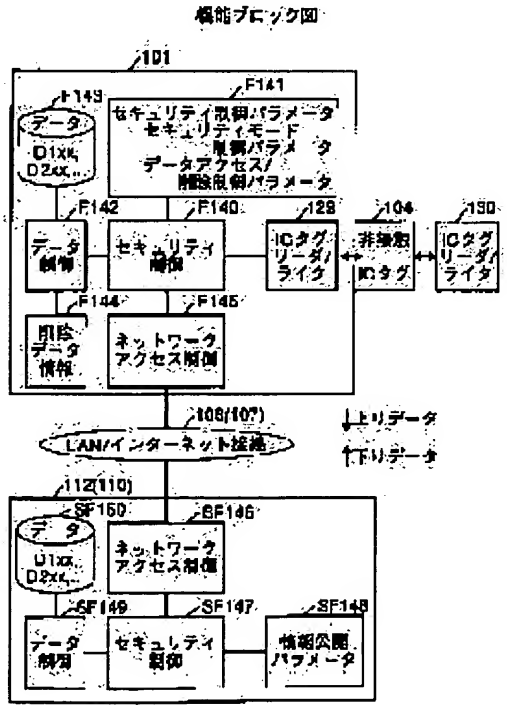
(72)Inventor : TADANO TORU
NAKAZAWA NOBUHIRO
FURUYAMA MIKIO

(54) INFORMATION SECURITY MANAGEMENT METHOD, PROGRAM FOR EXECUTING IT, AND INFORMATION SECURITY MANAGEMENT DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To apply information security according to a usage area (location) of a portable computer PC for preventing leakage of information.

SOLUTION: In use of the portable computer PC100 (PC012) transferred between the usage areas S101, S201, and S301, information operation by the computer is restricted in compliance with the usage area of the computer PC100 (PC012). In this case, the information operation is restricted differently in a plurality of divided usage areas S101, S201, and S301. In servers 112 and 110 connected to each other via the computer PC100 (PC012) and networks 106 and 107, information matching the usage areas of the computer is provided, and according, to the usage area of the computer, an offer of information to the computer is restricted.



LEGAL STATUS

[Date of request for examination]	12.01.2005
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－288275
（P2003－288275A）
(43)公開日　平成15年10月10日(2003.10.10)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
G06F	12/14	320	G06F	12/14	320F　5B017
	15/00	330		15/00	330A　5B035
G06K	17/00		G06K	17/00	L　5B058
	19/00			19/00	T　5B085

審査請求　未請求　請求項の数5　ＯＬ　（全 11 頁）

(21)出願番号　特願2002－93169(P2002－93169)

(22)出願日　平成14年３月28日(2002.3.28)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　只野　徹
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

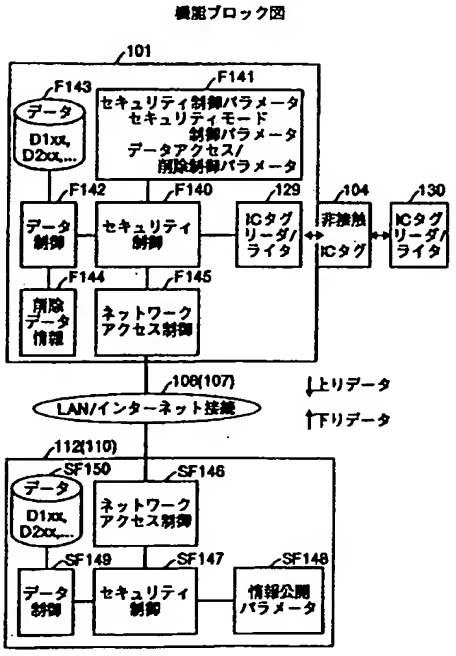
(72)発明者　中澤　信弘
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(74)代理人　100089118
弁理士　酒井　宏明

最終頁に続く

(54)【発明の名称】　情報セキュリティ管理方法、この方法を実行するプログラム、及び情報セキュリティ管理装置

(57)【要約】
【課題】　情報の漏洩を防止するためＰＣの使用エリア（場所）に応じて情報のセキュリティを施すようにしたこと。
【解決手段】　可搬性あるコンピュータＰＣ１００（ＰＣ０１２）を使用エリアをＳ１０１、Ｓ２０１、Ｓ３０１という具合に移動して使用するに当たり、コンピュータＰＣ１００（ＰＣ０１２）の使用エリアに応じてこのコンピュータによる情報操作に制限を加えるようにした。この場合、複数に区画された使用エリアＳ１０１、Ｓ２０１、Ｓ３０１に対してそれぞれ異なる情報操作の制限を行うようにした。また、コンピュータＰＣ１００（ＰＣ０１２）とネットワーク１０６、１０７を通じて接続されるサーバ１１２、１１０上にコンピュータの使用エリアに対応する情報を有し、コンピュータの使用エリアに応じてこのコンピュータへの情報の提供を制限する。



1

【特許請求の範囲】

【請求項１】　可搬性あるコンピュータを使用エリアを移動して使用するに当たり、コンピュータの使用エリアに応じてこのコンピュータによる情報操作に制限を加える情報セキュリティ管理方法。

【請求項２】　複数に区画された使用エリアに対してそれぞれ異なる情報操作の制限を行うことを特徴とする請求項１に記載の情報セキュリティ管理方法。

【請求項３】　可搬性あるコンピュータを使用エリアを移動して使用するに当たり、このコンピュータとネットワークを通じて接続されるサーバ上にコンピュータの使用エリアに対応する情報を有し、コンピュータの使用エリアに応じてこのコンピュータへの情報の提供を制限する情報セキュリティ管理方法。

【請求項４】　コンピュータの使用エリアを検出し、その使用エリアに応じてこのコンピュータによる情報操作に制限を加える方法をコンピュータに実行させるプログラム。

【請求項５】　使用エリアに対応してエリア固有信号を出力する発信機を備え、
この発信機からのエリア固有信号を受信する受信機を有しかつこの受信機により受信したエリア固有信号に応じて情報操作の制限を行う制御回路を有するコンピュータを備えた情報セキュリティ管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、可搬性あるコンピュータの使用エリアに応じて情報の操作あるいは情報の提供を制限（逆にいえば開放）する情報セキュリティ管理方法、この方法を実行するプログラム、及び情報セキュリティ管理装置に関する。

【０００２】

【従来の技術】従来、いわゆるセキュリティシステムは、多くの場所で種々存在し、例えば人の入退室や入退場を制限する人に対するもの、機器の持ち込みや持ち出しを制限する物に対するものが有り、更にはコンピュータやネットワークの分野でのデータやデータ処理に限れば、ＩＤ／パスワードやファイルのアクセス制限などコンピュータ単体に関するもの、利用者認証やネットワーク接続経路などサーバデータに関するものが、現実に挙げられる。

【０００３】このようなセキュリティシステムにあっては、コンピュータに係るデータ授受及びデータ処理などの情報操作に関するセキュリティは、ＩＤ／パスワード等概ね使用者に依存しているのが実状である。従って、使用者の個人認証さえできれば、コンピュータをどこに運んでどこで使用しようがまったく問題はない。殊にネットワークが張り巡らされてどこでもデータの授受やデータの処理が可能となり、一方ノートブック型パーソナルコンピュータ等可搬性あるパーソナルコンピュータ

2

（以下ＰＣという）が普及する現在、使用者個人のログインさえできればデータの取り出しやデータの処理等ＰＣによる作業はどこにおいても行える。

【０００４】

【発明が解決しようとする課題】しかしながら、このような状況においては情報漏洩が問題であり、そしてその最大の原因は、使用者によるものであることを勘案すると、使用者個人の個人認証だけでは情報のセキュリティは不十分である。具体的に例えばＰＣを外部へ持ち出し、使用者がログインさえできれば情報の取り出し等を容易に行うことができ、ＰＣを故意に持ち出されて悪用されることが十分考えられる。また、例えば可搬性あるＰＣであって常時ネットワークに接続されたＰＣにあって、人事異動などによりＰＣの使用場所が変更された場合には、新たな場所でのセキュリティシステムの変更や指導がネットワーク／サーバ管理者にて行われるが、個人認証だけに依存したのではこの変更や指導までのタイムラグによりセキュリティホールが発生する可能性もある。

【０００５】いずれにしても使用者個人による個人認証に依存して、情報のセキュリティを保持することは不十分である。

【０００６】この発明は、上述した従来技術による問題点を解消するためになされたものであり、ＰＣの使用エリア（場所）に応じて情報のセキュリティを施すようにした情報セキュリティ管理方法、この方法を実行するプログラム、及び情報セキュリティ管理装置を提供することを目的とする。

【０００７】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、請求項１の発明に係る情報セキュリティ管理方法は、ノートブック型あるいはデスクトップ型に係わらず可搬性あるコンピュータを使用エリアを移動して使用するに当たり、コンピュータの使用エリアに応じてこのコンピュータによる情報操作（例えばデータの授受やデータの処理）に制限（セキュリティモードの変更やアクセスの制限あるいはデータの削除）を加えることを特徴とする。

【０００８】この請求項１の発明によれば、コンピュータの使用エリアに応じたセキュリティ対策をとることができる。また、リスクの大小によりセキュリティと操作性との関係を適切に融合させることができる。

【０００９】また、請求項２の発明に係る情報セキュリティ管理方法は、請求項１の発明において、複数に区画された使用エリアに対してそれぞれ異なる情報操作の制限（セキュリティモードの変更やアクセスの制限あるいはデータの削除）を行うことを特徴とする。

【００１０】この請求項２の発明によれば、複数のエリアのリスクの段階に応じたセキュリティ対策をとることができる。

【００１１】また、請求項３の発明に係る情報セキュリティ管理方法は、可搬性あるコンピュータを使用エリアを移動して使用するに当たり、このコンピュータとネットワークを通じて接続されるサーバ上にコンピュータの使用エリアに対応する情報を有し、コンピュータの使用エリアに応じて情報公開パラメータを用いてこのコンピュータへの情報の提供を制限することを特徴とする。

【００１２】この請求項３の発明によれば、コンピュータの使用エリアに対応するネットワークのサーバ上にある情報の漏洩も防止することができる。

【００１３】また、請求項４の発明に係る情報セキュリティ管理方法を実行するプログラムは、コンピュータの使用エリアを検出し、その使用エリアに応じてこのコンピュータによる情報操作に制限を加えるアプリケーションプログラムとしたことを特徴とする。

【００１４】この請求項４の発明によれば、コンピュータ制御プログラムとしてセキュリティ制御プログラムを得ることができる。

【００１５】また、請求項５の発明に係る情報セキュリティ管理装置は、使用エリアに対応してエリア固有信号（エリア特定信号を含む）を出力する発信機を備え、この発信機からのエリア固有信号を受信する受信機を有しかつこの受信機により受信したエリア固有信号に応じて情報操作の制限を行う制御回路を有するコンピュータを備えたことを特徴とする。

【００１６】この請求項５の発明によれば、コンピュータの盗難や持ち出しに対しても有効なセキュリティ対策を講ずることができる。

【００１７】

【発明の実施の形態】以下に添付図面を参照して、この発明に係る情報セキュリティ管理方法、この方法を実行するプログラム、及び情報セキュリティ管理装置の好適な実施の形態を詳細に説明する。

【００１８】（実施の形態）まず、本実施の形態に係る情報セキュリティ管理方法、この方法を実行するプログラム、及び情報セキュリティ管理装置の前提となるコンピュータシステムについて説明する。図１は、コンピュータシステムの構成図であり、図２はコンピュータシステムのブロック図である。

【００１９】同図に示すように、図１に示すコンピュータシステムには、可搬性あるノートブック型ＰＣ１００の本体部１０１、本体部１０１からの指示により表示画面に画像等の情報を表示するディスプレイ１０２、このコンピュータシステムに種々の情報を入力するためのキーボード１０３、本体部１０１の外箱表面に貼付された非接触のＩＣタグ１０４、ディプレイ１０２の表示画面上の任意の位置を指定するマウス１０５、ローカルエリアネットワーク（ＬＡＮ）１０６または広域エリアネットワーク（ＷＡＮ）に接続するＬＡＮインターフェース、インターネットなどの公衆回線１０７に接続するモデム１０８、が備えられている。ここで、ＬＡＮ１０６は、ほかのコンピュータシステム１１１、サーバ１１２、プリンタ１１３等とＰＣ１００とを接続しており、公衆回線１０７もサーバ１１０とモデム１０８とを接続している。また、図２に示すように、本体部１０１は、ＣＰＵ１２１、ＲＡＭ１２２、ＲＯＭ１２３、ハードディスクドライブ（ＨＤＤ）１２４、ＣＤ－ＲＯＭドライブ１２５、ＦＤドライブ１２６、Ｉ／Ｏインターフェース１２７、ＬＡＮインターフェース１２８、及びＩＣタグリーダ１２９を備えている。なお、このＩＣタグリーダは、後述のＩＣタグライタと共用できる同じ製品すなわちＩＣタグリーダ／ライタを用いることができる。

【００２０】このコンピュータシステムにおいて使用エリアの情報セキュリティ管理を行おうとする場合、まず、そのエリア（場所）の出入口等に備えられた発信機であるＩＣタグライタ（図１、２では図示省略）によってＰＣ１００の本体部１０１に貼付されたＩＣタグ１０４にコードが書き込まれる。そして、このコードは、本体部１０１内に備えられたＩＣタグリーダ１２９にて読み出される。すなわち、ＰＣ１００にはそのＰＣ１００が存在するエリアのＩＣタグライタ１３０のコードが読み出されることになる。ＩＣタグリーダ１２９にて読み出されたコードは、Ｉ／Ｏインターフェース１２７を介してＲＡＭ１２２に記憶され、ＣＰＵ１２１にてエリア（場所）コードに変換されＲＡＭ１２２に記憶される。本体部１０１ではこのエリアコードに応じて情報セキュリティ制御が行われる。この情報セキュリティ制御は、例えばＨＤＤ１２４にて駆動されるハードディスクに記録されたセキュリティモード制御パラメータあるいはデータアクセス／削除制御パラメータに基づいてセキュリティモードを設定したりデータアクセスを制限したりあるいはデータの削除をするという制御である。また、図１及び図２に示すように本体部１０１が、ＬＡＮ１０６や公衆回線１０７を通じてサーバ１１２や１１０に接続されている場合には、前述の各本体部１０１に読み込まれたエリアコードに応じた情報セキュリティ制御により、サーバ内の情報公開パラメータに基づきサーバからの情報公開（提供）を制限するという制御も行われる。以上が図１、図２に示すコンピュータシステムを用いた情報セキュリティ管理の概要である。

【００２１】次に図３に示す機能ブロックを用いて情報セキュリティ管理装置の詳細を説明する。図３は、図２に示すブロックを情報セキュリティ制御の機能ブロックとして置き換えた図である。図３において、エリア（場所）の出入口等には発信機であるＩＣタグライタ１３０が備えられる。このＩＣタグライタ１３０では、書き込み機能にてライタ固有のコードが発信され、換言すればそのＩＣタグライタ１３０が置かれたエリア固有のコードが発信される。

【００２２】他方、ＰＣ１００の本体部１０１に貼付さ

れたＩＣタグ１０４には、ＩＣタグライタ１３０に近付いたりあるいは通過することによってこのライタ固有コードが書き込まれる。すなわち、ＰＣ１００を出入口等にて移動させたり通過させることにより非接触のＩＣタグ１０４に上記固有コードが書き込まれる。

【００２３】ＰＣ１００の本体部１０１内では、ＩＣタグ１０４に書き込まれた固有コードを読み出すためのＩＣタグリーダ１２９が備えられる。セキュリティ制御ブロックＦ１４０では、このＩＣタグリーダ１２９で読み出された固有コードに基づき、セキュリティモードの変更、データアクセス制限の変更、あるいはデータ削除の可否選択からなるセキュリティ制御が行われる。この場合、セキュリティモードの変更、データアクセス制限の変更、あるいはデータ削除の可否選択は、セキュリティ制御パラメータブロックＦ１４１によるパラメータに基づく。ここで、セキュリティモードの変更は、具体的にはＩＤ、パスワード、あるいはハードディスクパスワード等の選択をいい、データアクセス制限の変更は、例えば秘密の段階に応じたデータへのアクセスの段階的な制限の変更をいい、データの削除の可否選択は、データを削除するかあるいはしないかの選択をいう。

【００２４】なお、ＩＣタグライタ１３０の固有コードのコピーした場合にはこのセキュリティ制御は無効になるので、秘密の段階が高いＩＣタグライタ１３０には例えば暗号化キーを持たせＰＣ１００内にて複合化キーを持たせるようにしても良い。

【００２５】また、ＩＣタグライタ１３０の固有コードを書き込んだＩＣタグ１０４の固有コードをＩＣタグリーダ１２９にて読み出した状態では、ＰＣ１００の使用エリアは特定されないので、エリアを特定するテーブルとかアプリケーションプログラムを備えて複合化キーの照合と共にエリアコードを得るようにしても良い。また更に、ＩＣタグライタ１３０の固有コード自体をエリア特定コードとすることも可能であり、この場合にはエリア特定のためのテーブルやアプリケーションは不要となる。

【００２６】データ制御ブロックＦ１４２は、セキュリティ制御ブロックＦ１４０の制御情報に応じてデータファイルＦ１４３に対するデータ制御を行うもので、ＩＤ等が一致してもアクセス制限があれば例えば部分的にしかデータのアクセスができず、更にデータの削除の場合には削除データ情報を記録ブロックＦ１４４に記録するというデータ制御を行うものである。なお、削除データ情報記録ブロックＦ１４４は、データの削除にてデータを消し去るのではなく、ＰＣ１００の使用エリアがデータ削除の使用エリアから変化した場合、削除データを復旧させるために備えられたものである。

【００２７】また、ネットワークアクセス制御ブロックＦ１４５は、セキュリティ制御ブロックＦ１４０の制御情報に応じてネットワーク１０６や１０７に対するアクセス制御を行うもので、例えばＩＤ等が一致しなければネットワークへのアクセスはできない。

【００２８】一方、サーバ１１２や１１０でも同様に機能ブロックを有し、ネットワークアクセス制御ブロックＳＦ１４６はネットワーク１０６や１０７に対するアクセス制御を行う。セキュリティ制御ブロックＳＦ１４７では、ＰＣ１００でのセキュリティ制御ブロックＦ１４０でのセキュリティ制御に応じてセキュリティ制御を行うもので、例えばアクセス制限があれば情報公開パラメータブロックＳＦ１４８のパラメータに基づく部分的なアクセスしかできず、情報の部分的な提供しかできないようになっている。データ制御ブロックＳＦ１４９は、セキュリティ制御ブロックＳＦ１４７の制御情報に応じてデータファイルＳＦ１５０に対するデータ制御を行うものである。なお、図３においては、ＰＣ１００のネットワーク１０６や１０７への接続を前提として説明したが、ＰＣ１００を単独で使用する場合にはサーバ１１２や１１０への情報公開パラメータのアクセス制限は存在しない。

【００２９】図４は、ＰＣ１００の使用エリアとして一つの部屋Ｓ５０１を想定し、この部屋Ｓ５０１にＰＣ１００を持ち込んだり持ち出したりするケースを示している。すなわち、通常ＰＣ１００を使用する部屋Ｓ５０１では、使用者の個人認証のみにて何らアクセスの制限なく使用できる場合でも、このＰＣ１００を出入口を通って持ち出そうとした場合には出入口付近に設置されたＩＣタグライタ１３０ｉ及び１３０ｅから送信される固有コードによりＰＣ１００内のセキュリティ制御が実行され、例えばＰＣ１００内のデータファイルＦ１４３のデータを削除データとして、部屋Ｓ５０１外のＰＣ１００ではデータの取り出しや処理を不可能にすることができる。また逆に、部屋Ｓ５０１内のＰＣ１００を一旦部屋Ｓ５０１外に出したが再度部屋Ｓ５０１内に運び込む場合には、ＩＣタグライタ１３０ｉ及び１３０ｅから送信される固有コードにより削除データとするセキュリティ制御が外れ元のまま使用者の個人認証のみにて何らアクセスの制限なく使用できるようにもできる。また、外部から別の場所のＰＣ１００が持ち込まれた場合には、新品のＰＣを除いて、ＬＡＮに接続した場合、サーバ１１２からのデータを削除データとするセキュリティ制御をしても良い。このように同じＰＣ１００の同じエリアへの持ち出しや持ち込みを繰り返す場合には、固有コードの履歴を見ることによって、セキュリティ制御を実行したり外すことでエリアのセキュリティの保持と復旧が可能になる。

【００３０】ここで、セキュリティ制御の実行時期は、ＰＣ１００の移動後ＰＣ１００の起動時であったり、あるいはＰＣ１００の起動中定期的に行うことができる。

【００３１】また、部屋Ｓ５０１の出入口付近に備えたＩＣタグライタ１３０ｉ、１３０ｅは出入口の内と外と

に備えたが、これはＰＣ１００の出入口の通過の確認と移動の方向の確認のためのものであり、ＰＣ１００のＩＣタグ１０４にＩＣタグライタ１３０ｉと１３０ｅとの内外双方のコードが記録されれば通過となり、この場合１３０ｉの固有コードが先に記録され１３０ｅの固有コードが後の場合は持ち出し、逆の場合は持ち込みとなる。また、片方のＩＣタグライタ１３０ｉあるいは１３０ｅのみの固有コードの記録の場合はそのＩＣタグライタ側のエリアにＩＣタグすなわちＰＣ１００が存在することになる。この出入口内外のＩＣタグライタ１３０ｉと１３０ｅ双方の配置は、近づくことによってＩＣタグ１０４にコードが記録される種類のＩＣタグにとって、通過と移動方向の両者を記録するには有効である。もっとも、一つのＩＣタグライタ１３０でもＰＣ１００の通過と移動方向が記録でき伴別できるＩＣタグ１０４の場合には、すなわち通過することによってのみ移動方向が記録されるＩＣタグ１０４の場合には、ＩＣタグライタを二つ備える必要はない。このようにＩＣタグライタは固有コードを発信し、その固有コードをＩＣタグは記録するものであるが、要はＩＣタグ引いてはＰＣ１００の存在位置がＩＣタグライタの固有コードによって特定できれば良い。

【００３２】図５は、ＰＣ１００の使用エリアとして三つの部屋Ｓ１０１(関係者外秘エリア)、Ｓ２０１(社内事務エリア：顧客立入り不可エリア)、Ｓ３０１（社内オープンエリア：顧客立入り可エリア）と外部エリアＳ２０２(外部事務所の事務エリア)を想定し、この部屋Ｓ１０１からＰＣ１００を持ち出すケースを示している。なお、この図５に示す例でも図４の説明が基礎となっている。すなわち、ＰＣ１００の持ち出しのみならず持ち込みもあること、持ち出しと持ち込みの繰り返しもあること、セキュリティ制御の実行時期は起動時も起動中の定期的な時でもよいこと、ＩＣタグライタ１３０とＩＣタグ１０４との方式は近づくことで記録したり通過することで記録する方式があること、については、図５の例でも準じて適用される。

【００３３】この図５の例では、主にセキュリティ制御の詳細について述べる。この例では、図４の例と同じようにＩＣタグライタは部屋Ｓ１０１、Ｓ２０１、Ｓ３０１の出入口の内外両側に設けられる例を示している。今、ＰＣ１００が、部屋Ｓ１０１から部屋Ｓ２０１を経て部屋Ｓ３０１に至る場合を述べる。この図５では、便宜上ＰＣ１００をそのコードＰＣ０１２で表し、ＩＣタグ１０４をそのコードＩＣ１２３にて表し、ＩＣタグライタ１３０ｉ及び１３０ｅをそのコードＧ１ｉ、Ｇ１ｅ、Ｇ２ｉ、Ｇ２ｅ、Ｇ３ｉ、Ｇ３ｅ、Ｇ４ｉ、Ｇ４ｅにて表す。

【００３４】図５において、部屋Ｓ１０１に存在するＰＣ０１２は部屋Ｓ１０１の出入口の通過にて固有コードＧ１ｉ、Ｇ１ｅがＩＣ１２３のタグに記憶され、ついで

次の出入口の通過にて固有コードＧ２ｉ、Ｇ２ｅがＩＣ１２３のタグに記憶される。この状態では、ＰＣ０１２は部屋Ｓ３０１に存在する。この経過を図６に示すデータ構造図上、（Ａ）ＩＣタグに関する履歴ではタグＩＣ１２３にてコードＧ１ｉ、Ｇ１ｅが記録されてＰＣ０１２内では部屋Ｓ１０１からＳ２０１への移動が確認され、更にコードＧ２ｉ、Ｇ２ｅが記録されてＰＣ０１２内では部屋Ｓ２０１からＳ３０１への移動が確認される。従って、ＰＣ０１２のセキュリティ制御ブロックＦ１４０ではエリアコードＳ２０１そしてＳ３０１(便宜上部屋の符号とエリアコードを同じ表示とする)が入力される。

【００３５】ＰＣ０１２がこのような経過を辿る移動をすることによって、セキュリティモードを変更する場合、図６のデータ構造図上、（Ｂ）セキュリティモード変更パラメータでは、エリアコードＳ１０１にてモードＭ１の特定個人の「ＩＤ」入力要、エリアコードＳ２０１ではモードＭ２の「無し」である認証不要、エリアコードＳ３０１ではモードＭ３の「ＩＤ／パスワード」入力要、というようなモード変更が行われる。なお、このセキュリティモード変更パラメータでは、エリアコードＳ４０１ではモードＭ４の「ＩＤ／パスワード／ハードディスクパスワード」入力要、エリアコード不明（ＩＣタグが剥がれる等）では起動不可というモード変更となっている。

【００３６】また、ＰＣ０１２がこのような移動をすることによって、データアクセス制限やデータの削除をする場合、図６のデータ構造図上、（Ｃ）データアクセス／削除制御パラメータでは、エリアコードによってアクセスが可能あるいは不可能なデータコード、並びに削除が要あるいは不要なデータコードが選択される。また、図６（Ｄ）に基づけばデータコードＤ１では顧客信用調査情報等の関係者外秘情報、データコードＤ２では顧客取引情報等の社外秘情報、データコードＤ３では顧客担当者情報等の社外持ち出し禁止情報、データコードＤ４では顧客公開情報等の公開情報が対応する。従って、図６（Ｃ）によれば、データコードＤ１、Ｄ２、Ｄ３、Ｄ４について、エリアコードＳ１０１は全データコードＤ１、Ｄ２、Ｄ３、Ｄ４にアクセス可能で削除は要しないエリアであり、エリアコードＳ２０１はデータコードＤ１につきアクセス不可能あるいは削除を要しかつデータコードＤ２、Ｄ３、Ｄ４につきアクセス可能あるいは削除は要しないエリアであり、エリアコードＳ３０１はデータコードＤ１、Ｄ２につきアクセス不可能あるいは削除を要しかつデータコードＤ３、Ｄ４につきアクセス可能あるいは削除は要しないエリアである。更に、エリアコードＳ４０１はデータコードＤ１、Ｄ２、Ｄ３につきアクセス不可能あるいは削除を要しかつデータコードＤ４につきアクセス可能あるいは削除は要しないエリアであり、エリアコード不明では全データコードＤ１、Ｄ

２、Ｄ３、Ｄ４につきアクセス不可能あるいは削除を要する非常事態となっている。こうして、ＰＣ０１２が社外に至るに従い、アクセスが不可能な情報が増え、削除を要する情報が増大する。

【００３７】ここで、一般に秘密の要求が高い情報は操作性が煩雑で管理も厳重となり、逆に公開性の高い情報は操作しやすく管理も容易となるのであるが、これまで一般に行われてきたセキュリティ対策は、秘密の要求が高い情報に対して必要以上に操作性を悪くしたり管理負荷が過度であったり、反面に秘密の要求が高い情報であっても、操作性を優先するあまり脆弱となっているという状況が見受けられる。本実施の形態では、図５での部屋の構成に基づいて図６（Ｂ）（Ｃ）の制御パラメータを設定しており、これらの説明から判明するように例えば情報漏洩のリスクが大きければセキュリティを優先し、このリスクが少なければ操作性を優先するというセキュリティと操作性とのトレードオフの関係を適切に融合させている。

【００３８】図７（Ａ）は、ＰＣ０１２が使用エリアを移動することによって削除すべきデータ情報の履歴を示したもので、エリアコードに対応してデータコードが削除される。すなわち、エリアコードＳ２０１が得られる場合つまり部屋Ｓ２０１にＰＣ０１２が移動した時データコードＤ１の情報が削除される。更に、部屋Ｓ３０１にＰＣ０１２が移動してエリアコードＳ３０１となった時はデータコードＤ２の情報が削除される。この図７の削除データの履歴は、図６（ｃ）に示す削除制御パラメータのデータ構造とも一致している。

【００３９】図７（Ｂ）はＰＣ０１２が移動した後ネットワークに接続した場合、サーバ側での情報公開パラメータを示しており、ＰＣ０１２の移動により得られたエリアコードに対応して図７（Ｃ）に示すデータコードを選択して公開可能あるいは不可能としたり、削除した場合には復元可能あるいは不可能とするものである。この場合、削除データを復元可能とすることは、エリアデータの変更にて削除されていたデータをＰＣ０１２からの復元要求にてアクセス可能とし復元データを公開（提供）することである。この図７（Ｂ）の情報公開パラメータ及び図７（Ｃ）のデータコードの内容は、図６（Ｃ）（Ｄ）と同じであり説明は省略する。

【００４０】図８（Ａ）は、セキュリティ制御での制御処理を示したフローチャートである。図８（Ａ）において、まずＩＣタグに書き込まれた固有コードからエリアコードを求め（ステップＳＴ１）、次いで電源起動時のセキュリティ制御の場合には、セキュリティコードに対応するセキュリティモードを起動する（ステップＳＴ２）。ステップＳＴ３にてデータ制御がない場合は、フローの終了となるが、データ制御を行う場合には、ステップＳＴ４にてデータの削除があるかどうかの判断をする。データの削除がない場合には、アクセス制御であるので、エリアコードに対応するアクセス不可データのアクセスを禁止する（ステップＳＴ５）。一方データの削除がある場合には、エリアコードに対応する削除データを削除し削除データ情報に書き込む（ステップＳＴ６）。なおこのフローチャートで電源起動時のセキュリティ制御をしないで、定期的なセキュリティ制御にチェックを行う場合には、ステップＳＴ２は不要となる。

【００４１】図８（Ｂ）はＩＣタグからのコード書き込みフローチャートを示し、まずＩＣタグライタからＩＣタグにゲート情報である固有コードが書き込まれる（ステップＳＴ１０）。次いで、本体内にて固有コードから対応するエリアコードに変換する（ステップＳＴ１１）。この後セキュリティ制御が実行される（ステップＳＴ１２）。

【００４２】上述してきたように、本実施の形態１では、ＩＣタグライタ１３０、ＩＣタグ１０４、ＩＣタグリーダ１２９によって固有コードを得てセキュリティ制御を行うものであったが、ＧＰＳの衛星からの送信信号を受信する受信機をＰＣに搭載すれば、この位置情報もしくは、位置情報と時刻との組合せを利用して、ＰＣの使用エリアを特定することによってセキュリティ制御を行うことができる。この場合、位置情報に正確を期すためにディファレンシャルＧＰＳを適用することも可能である。

【００４３】なおここでは、ＰＣ０１２の使用エリアを検出し、その使用エリアに応じてこのＰＣ０１２による情報操作に制限を加える方法を実行させるプログラム、つまり図３の機能を前提として図６、図７に基づき図８のフローチャートをコンピュータに実行させるプログラムを得ることができる。

【００４４】本実施の形態によれば、ＰＣ０１２の使用エリア（場所）に応じて情報操作に制限を加えるようにできたので、ＰＣ０１２の使用エリアとセキュリティの段階に応じた情報のセキュリティ制御を行うことができた。

【００４５】（付記１）可搬性あるコンピュータを使用エリアを移動して使用するに当たり、コンピュータの使用エリアに応じてこのコンピュータによる情報操作に制限を加えることを特徴とする情報セキュリティ管理方法。

【００４６】（付記２）複数に区画された使用エリアに対してそれぞれ異なる情報操作の制限を行うことを特徴とする付記１に記載の情報セキュリティ管理方法。

【００４７】（付記３）コンピュータによる情報操作の制限はセキュリティモードを変更して行うことを特徴とする付記１または２に記載の情報セキュリティ管理方法。

【００４８】（付記４）コンピュータによる情報操作の制限はデータアクセスを制限して行うことを特徴とする付記１または２に記載の情報セキュリティ管理方法。

11

【００４９】（付記５）コンピュータによる情報操作の制限はデータを削除して行うことを特徴とする付記１または２に記載の情報セキュリティ管理方法。

【００５０】（付記６）削除したデータは、コンピュータの使用エリアに応じて復旧可能としたことを特徴とする付記５に記載の情報セキュリティ管理方法。

【００５１】（付記７）コンピュータの使用エリアの特定は、使用エリアに対応して発信機から出力されるエリア特定信号であることを特徴とする付記１または２に記載の情報セキュリティ管理方法。

【００５２】（付記８）コンピュータの使用エリアの特定は、ＧＰＳの衛星から送られた受信信号に基づいて行うことを特徴とする付記１または２に記載の情報セキュリティ管理方法。

【００５３】（付記９）コンピュータの使用エリアの特定は、コンピュータ起動時に行うことを特徴とする付記１または２に記載の情報セキュリティ管理方法。

【００５４】（付記１０）コンピュータの使用エリアの特定は、コンピュータ起動中周期的に行うことを特徴とする付記１または２に記載の情報セキュリティ管理方法。

【００５５】（付記１１）可搬性あるコンピュータを使用エリアを移動して使用するに当たり、このコンピュータとネットワークを通じて接続されるサーバ上にコンピュータの使用エリアに対応する情報を有し、コンピュータの使用エリアに応じてこのコンピュータへの情報の提供を制限する情報セキュリティ管理方法。

【００５６】（付記１２）コンピュータへの情報の提供の制限は、セキュリティモードに応じて行うことを特徴とする付記１１に記載の情報セキュリティ管理方法。

【００５７】（付記１３）コンピュータへの情報の提供の制限は、データアクセスを制限して行うことを特徴とする付記１１に記載の情報セキュリティ管理方法。

【００５８】（付記１４）コンピュータへの情報の提供の制限は、データを削除して行うことを特徴とする付記１１に記載の情報セキュリティ管理方法。

【００５９】（付記１５）削除したデータは、コンピュータの使用エリアに応じて復旧可能としたことを特徴とする付記１４に記載の情報セキュリティ管理方法。

【００６０】（付記１６）コンピュータへの情報の提供の制限は、使用エリアに対応して発信機から出力されるコンピュータからのエリア特定信号に基づいて行うことを特徴とする付記１１に記載の情報セキュリティ管理方法。

【００６１】（付記１７）コンピュータへの情報の提供の制限は、コンピュータから送られるＧＰＳからの受信信号に基づいて行うことを特徴とする付記１１に記載の情報セキュリティ管理方法。

【００６２】（付記１８）コンピュータの使用エリアを検出し、その使用エリアに応じてこのコンピュータによる情報操作に制限を加える情報セキュリティ管理方法をコンピュータに実行させるプログラム。

12

【００６３】（付記１９）コンピュータによる情報操作の制限はセキュリティモードを変更して行うことを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記１８に記載のプログラム。

【００６４】（付記２０）コンピュータによる情報操作の制限はデータアクセスを制限して行うことを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記１８に記載のプログラム。

【００６５】（付記２１）コンピュータによる情報操作の制限はデータを削除して行うことを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記１８に記載のプログラム。

【００６６】（付記２２）削除したデータは、コンピュータの使用エリアに応じて復旧可能としたことを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記２１に記載のプログラム。

【００６７】（付記２３）コンピュータの使用エリアは、使用エリアに対応して発信機から出力されるエリア特定信号を検出することを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記１８に記載のプログラム。

【００６８】（付記２４）コンピュータの使用エリアは、ＧＰＳの衛星から送られた受信信号に基づいて検出することを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記１８に記載のプログラム。

【００６９】（付記２５）コンピュータの使用エリアは、コンピュータの起動時に検出することを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記１８に記載のプログラム。

【００７０】（付記２６）コンピュータの使用エリアは、コンピュータの起動中周期的に検出することを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記１８に記載のプログラム。

【００７１】（付記２７）使用エリアに対応してエリア特定信号を出力する発信機を備え、この発信機からのエリア特定信号を受信する受信機を有しかつこの受信機により受信したエリア特定信号に応じて情報操作の制限を行う制御回路を有するコンピュータを備えた情報セキュリティ管理装置。

【００７２】（付記２８）発信機はＩＣタグリーダライタであり、受信機は非接触ＩＣタグである付記２７に記載の情報セキュリティ管理装置。

【００７３】（付記２９）ＧＰＳの衛星からの送信信号を受信する受信機を有し、この受信機によりコンピュータの使用エリアを特定しかつこの使用エリアに応じて情報操作の制限を行う制御回路を有するコンピュータを備えた情報セキュリティ管理装置。

【００７４】（付記３０）受信機はディファレンシャル

ＧＰＳに基づいて構成される付記２９に記載の情報セキュリティ管理装置。

【００７５】

【発明の効果】以上説明したように、請求項１の発明によれば、可搬性あるコンピュータを使用エリアを移動して使用するに当たり、コンピュータの使用エリアに応じてこのコンピュータによる情報操作に制限を加えることにより、コンピュータの使用エリアに応じたセキュリティ対策をとることができ、リスクの大小によりセキュリティと操作性との関係を適切に融合させることができるという効果を奏する。

【００７６】また、請求項２の発明によれば、複数に区画された使用エリアに対してそれぞれ異なる情報操作の制限を行うことにより、複数のエリアの段階に応じたセキュリティ対策をとることができるという効果を奏する。

【００７７】また、請求項３の発明によれば、可搬性あるコンピュータを使用エリアを移動して使用するに当たり、このコンピュータとネットワークを通じて接続されるサーバ上にコンピュータの使用エリアに対応する情報を有し、コンピュータの使用エリアに応じてこのコンピュータへの情報の提供を制限することにより、コンピュータの使用エリアに対応するネットワークのサーバ上にある情報の漏洩も防止することができるという効果を奏する。

【００７８】また、請求項４の発明によれば、コンピュータの使用エリアを検出し、その使用エリアに応じてこのコンピュータによる情報操作に制限を加えるプログラムであることにより、コンピュータ制御プログラムとしてセキュリティ制御プログラムを得ることができるという効果を奏する。

【００７９】また、請求項５の発明によれば、使用エリアに対応してエリア固有信号を出力する発信機を備え、この発信機からのエリア固有信号を受信する受信機を有しかつこの受信機により受信したエリア固有信号に応じて情報操作の制限を行う制御回路を有するコンピュータを備えたことにより、コンピュータの盗難や持ち出しに対しても有効なセキュリティ対策を講ずることができるという効果を奏する。

【図面の簡単な説明】

【図１】本実施の形態に係るコンピュータシステムの概略を示す構成図である。

【図２】本実施の形態に係る図１のコンピュータシステムのブロック図である。

【図３】本実施の形態に係る機能ブロック図である。

【図４】コンピュータの単一使用エリアを示す構成図である。

【図５】コンピュータの複数使用エリアを示す構成図である。

【図６】データ構造図である。

【図７】データ構造図である。

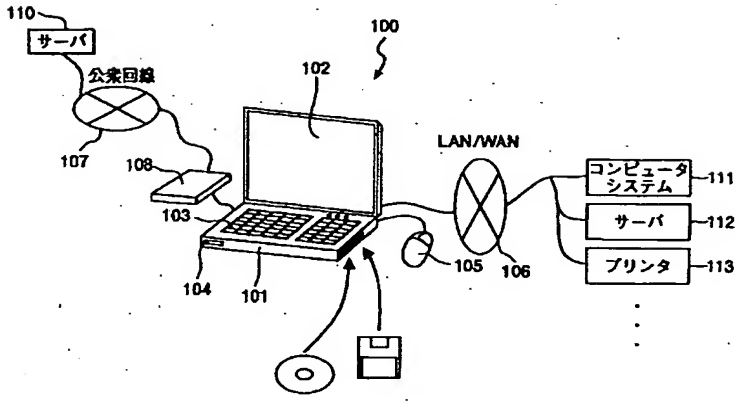
【図８】セキュリティ機能のフローチャートである。

【符号の説明】

１００、ＰＣ１００、ＰＣ０１２　コンピュータ
１０１　本体部
１０４　ＩＣタグ
１０６　ネットワーク
１０７　公衆回線
１１０、１１２　サーバ
１２９　ＩＣタグリーダ
１３０、１３０ｉ、１３０ｅ、Ｇ１ｉ、Ｇ１ｅ、Ｇ２ｉ、Ｇ２ｅ、Ｇ３ｉ、Ｇ３ｅ、Ｇ４ｉ、Ｇ４ｅ　ＩＣタグライタ
Ｆ１４０、ＳＦ１４７　セキュリティ制御ブロック
Ｆ１４１　セキュリティ制御パラメータブロック
Ｆ１４２、ＳＦ１４９　データ制御ブロック
Ｆ１４３、ＳＦ１５０　データファイル
Ｆ１４４　削除データ情報ブロック
ＳＦ１４８　情報公開パラメータブロック
Ｓ１０１、Ｓ２０１、Ｓ３０１、Ｓ２０２、Ｓ５０１　部屋
ＩＣ１２３、ＰＣ０１２、Ｓ１０１、Ｓ２０１、Ｓ３０１、Ｓ２０２、Ｇ１ｉ、Ｇ１ｅ、Ｇ２ｉ、Ｇ２ｅ、Ｇ３ｉ、Ｇ３ｅ、Ｇ４ｉ、Ｇ４ｅ、Ｍ１、Ｍ２、Ｍ３、Ｍ４、Ｄ１、Ｄ２、Ｄ３、Ｄ４　コード（なお、説明の便宜上ＰＣ０１２、Ｓ１０１、Ｓ２０１、Ｓ３０１、Ｓ２０２、Ｇ１ｉ、Ｇ１ｅ、Ｇ２ｉ、Ｇ２ｅ、Ｇ３ｉ、Ｇ３ｅ、Ｇ４ｉ、Ｇ４ｅ、はコードと装置（ここではＰＣ、部屋、ＩＣタグライタ）の表示を兼用する。）

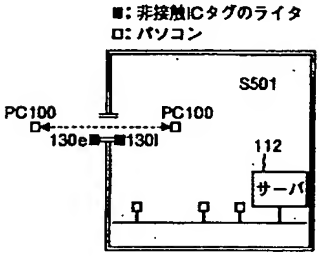
【図１】

コンピュータシステムの概略構成図



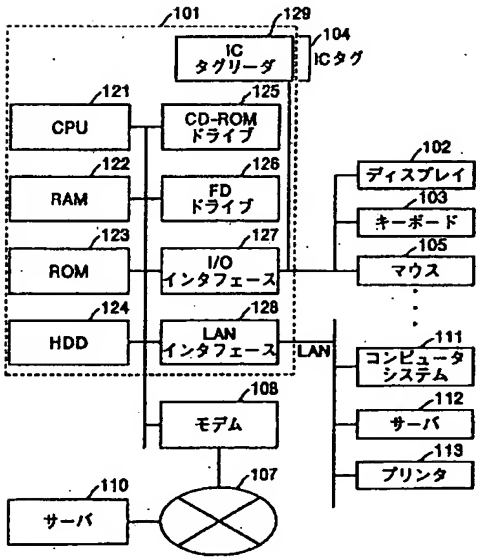
【図４】

単一使用エリアの構成図



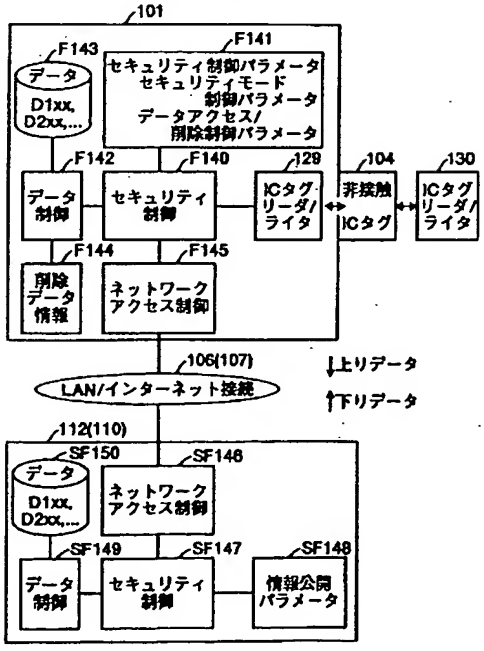
【図２】

コンピュータシステムのブロック図



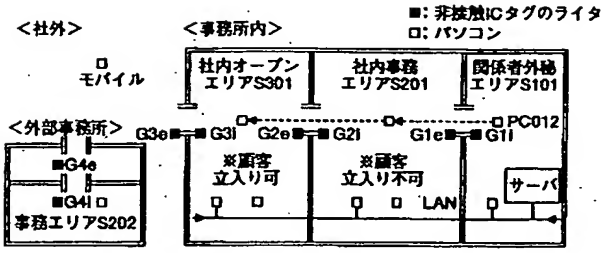
【図３】

機能ブロック図



【図５】

複数使用エリアの構成図



【図６】

データ構造図

(A) 非接触ICタグに関する属性

ICコード	PCコード	エリア情報 コード	エリア情報 名称	ゲート情報 コード	ゲート情報 年月日時分秒
IC123	PC012	S301	社内オープンエリア	G2e, G2i	020204103145
：	：	S201	社内事務エリア	G1e, G1i	020204090255
：	：	：	：	：	：

(B) セキュリティモード制御パラメータ

エリア コード	エリア 名称	セキュリティモード コード	セキュリティモードの例
S1xx	関係者外秘エリア	M1	ID入力
S2xx	社内事務エリア	M2	無し
S3xx	社内オープンエリア	M3	ID/パスワード入力
S4xx	社外エリア	M4	ID/パスワード、ハードディスクパスワード入力
不明	非常事態	XX	起動不可

(C) データアクセス/削除制御パラメータ

○：アクセス可、又は削除不要
×：アクセス不可、又は削除要

エリア エリア	エリア 名称	データコード D1	D2	D3	D4
S1xx	関係者外秘エリア	○	○	○	○
S2xx	社内事務エリア	×	○	○	○
S3xx	社内オープンエリア	×	×	○	○
S4xx	社外エリア	×	×	×	○
不明	非常事態	×	×	×	×

(D) データコードの例

コード	セキュリティレベル	情報の例
D1xx	関係者外秘	顧客信用調査情報
D2xx	社外秘	顧客取引情報
D3xx	社外持ち出し禁止	顧客担当者情報
D4xx	公開情報	顧客公開情報

【図７】

データ構造図

(A) 削除データ情報

ICコード	PCコード	削除情報 エリア	ファイル名	情報コード	年月日時分秒
IC123	PC012	S301	顧客取引情報	D2xx	020204104545
：	：	：	：	：	：
：	：	S201	顧客信用調査情報	D1xx	020204091530
：	：	：	：	：	：

(B) 情報公開パラメータ

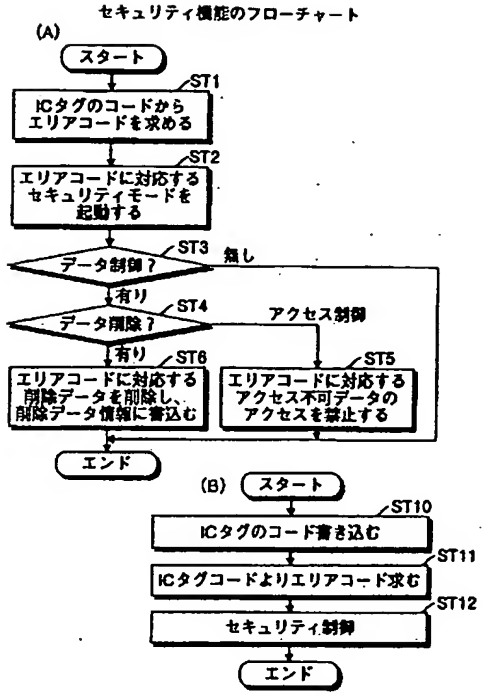
○：公開可、又は復元可
×：公開不可、又は復元不可

エリア コード	エリア 名称	データコード D1	D2	D3	D4
S1xx	関係者外秘エリア	○	○	○	○
S2xx	社内事務エリア	×	○	○	○
S3xx	社内オープンエリア	×	×	○	○
S4xx	社外エリア	×	×	×	○
不明	非常事態	×	×	×	×

(C) データコードの例

コード	セキュリティレベル	情報の例
D1xx	関係者外秘	顧客信用調査情報
D2xx	社外秘	顧客取引情報
D3xx	社外持ち出し禁止	顧客担当者情報
D4xx	公開情報	顧客公開情報

【図８】



フロントページの続き

(72)発明者　古山　幹雄
神奈川県川崎市中原区上小田中４丁目１番
１号　富士通株式会社内

Ｆターム(参考)　5B017 AA06 BB09 BB10
5B035 BB09 BC00 CA23
5B058 CA15 KA02 KA04 YA20
5B085 AE00 AE06 AE11